ABSTRACT

A system and method are disclosed for ensuring the security and integrity of a party's private key stored on a smartcard or other hardware token. A set of security requirements are defined for the smartcard that ensure that the card is manufactured and initialized in a secure environment and that it can withstand certain types of cryptographic and other attacks. The requirements further ensure that, at the conclusion of the initiation process, there exists only a single instance of the private key, thus decreasing the likelihood of a subsequent key compromise.